OMB Number 1670-0007
Expiration Date 2/29/08

Site Security Plan

A Site Security Plan (SSP) will be submitted by chemical facilities designated as high-risk by The Department of Homeland Security. The format of an SSP may vary, but each SSP must contain the following information:

1. Address each vulnerability identified in the facility's Security Vulnerability Assessment, and identify and describe the security measures to address each such vulnerability.
2. Identify and describe how security measures selected by the facility will address the applicable risk-based performance standards (see below) and potential modes of terrorist attack including, as applicable, vehicle-borne explosive devices, water-borne explosive devices, ground assault, or other modes or potential modes identified by the Department.
3. Identify and describe how security measures selected and utilized by the facility will meet or exceed each applicable performance standard listed at 6 CFR § 27.230 for the appropriate risk-based tier for the facility.
4. Specify other information the Assistant Secretary deems necessary regarding chemical facility security.

Risk-based Performance Standards
6 CFR § 27.230

1. **Restrict Area Perimeter**: Secure and monitor the perimeter of the facility.
2. **Secure Site Assets**: Secure and monitor restricted areas or potentially critical targets within the facility.
3. **Screen and Control Access**: Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter
4. **Deter, Detect, and Delay**: Create sufficient time between detection of an attack and the point at which the attack becomes successful.

5. **Shipping, Receipt, and Storage**: Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility.
6. **Theft and Diversion**: Deter theft or diversion of potentially dangerous chemicals.
7. **Sabotage**: Deter insider sabotage.
8. **Cyber**: Prevent unauthorized onsite or remote access to critical process controls, such as Supervisory Control and Access Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (ICS), critical business system, and other sensitive computerized systems.
9. **Response**: Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders.
10. **Monitoring**: Maintain effective monitoring, communications and warning systems.
11. **Training**: Ensure proper security training, exercises, and drills of facility personnel.
12. **Personnel Surety**: Perform appropriate background checks on ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets.
13. **Elevated Threats**: Escalate the level of protective measures for periods of elevated threat.
14. **Specific Threats, Vulnerabilities, or Risks**: Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue.
15. **Reporting of Significant Security Incidents**: To the Department and to local law enforcement officials.
16. **Significant Security Incidents and Suspicious Activities**: Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site.
17. **Officials and Organization**: Establish official(s) and an organization responsible for security and for compliance with these standards.
18. **Records**: Maintain appropriate records.
19. Address any additional performance standards the Assistant Secretary may specify.